A Review of Smart TV Forensics: Present State & Future Challenges

Mousa Al Falayleh
College of Computer Information Technology
American University in the Emirates (AUE)
P.O. Box: 503000, Dubai, United Arab Emirates
mousa.falayleh@aue.ae

ABSTRACT

Advance technology has given a new dimension to the field of entertainment and has expanded beyond one's imagination. Smart TV is one of these advance technology that has emerged before us with diverse features. Smart TV has become the next target for the cyber crimes. Smart TV Forensics is the science of recovering digital evidence from a smart TV under forensically sound conditions. This paper shed light on Smart TV Forensics and various challenges to face in its early childhood stage.

KEYWORDS

Digital Forensics, Cyber-Security, Smart TV, Smart TV Investigation.

1 INTRODUCTION

According to Cisco, more than 50 billion devices will be connected to the Internet of Things (Internet of Everything) by 2020. They even created a dynamic "connections counter" to track the estimated number of connected things until July 2020 [1]. These "things" may include mobile devices, parking meters, game consoles, cardiac monitors, smart cars, smart TVs, etc. Smart TV is the 21st century entertainment system that has given a versatile appearance to the world of entertainment behind the veil of technology. Smart TV is not just a TV, it is more focused on the higher online interactive media with software applications and Web widgets present in it like notebooks and smart phones. Smart TV is a combined term for a new generation TV units, also called set-top-boxes. It offers more advance computer ability and connectivity using the internet and it would not be wrong to call it information appliance [2]. The intelligent interaction feature of the TV allows the users to interact with it through voice, gestures or using remote control.

According to GARTNER [3], worldwide unit production of flat-panel smart TVs will grow from 69M in 2012 to 108M in 2013 to 198M in 2016. 85% of all flat-panel TVs produced in 2016 will be internet-connected smart TVs. The NPD GROUP predicts that 119M US TVs will be connected to the internet by 2015, up 51% from 2013.

The upcoming wide spread of smart TVs at houses and work places, will result in shifting the attention of hackers and intruders toward this new technology. Malta-based security start-up ReVuln claims to have discovered a zero-day vulnerability affecting Smart TV, in particularly a Samsung TV LED 3D. Exploits developed by ReVuln appear to allow it to access remote files and information, including viewing history,

as well as the ability to siphon off data on USB drives attached to a compromised TV [4].

This paper introduces a review of smart TV in general and its role in forensics in specific. It explores the present state and future challenges. It is organized as follows. Section 2 explores various usages and features of smart TVs. Section 3 discuss how criminals may use a smart TV to commit a cybercrime. Section 4 introduces smart TV forensics and various challenges that are facing this field. Finally, Section 5 gives some concluding remarks.

2 SMART TV

Smart TV also known as hybrid TV or connected TV, is the integration of the internet and the normal TV that gives it the capability to provide network related services. It is a web connected TV that uses processor and Ram like any notebook or desktop PC. It has built in software, web cameras are integrated within the system along with the sensors. In some, Wi-Fi could be used too for linking TV and internet but Wi-Fi does not support quality video [5]. Every manufacturer of the TV has introduced its own application store, through which the user can install, update or uninstall the application according to their needs and desire [6]. It uses Web 2.0 that facilitates in the interactive coverage and provides interactive experience for the users.

All the smart TV connections to the Internet use communication protocols to establish connectivity. The connections are tested and verified for any risks so that only secure connections could be established. Using internet they can provide wide range of online services.

There are various functions that the Smart TV can perform to facilitate its users in different ways. These functions are stated below:

1. Provides access to user granted content
2. Provides access to interactive services and applications
3. Access to network interfaces
4. Access to USB interfaces
5. Web browsing using keyboards and mouse support
6. Remote control applications for smart phones and tablets.
7. Video and audio interaction for the high end model
8. Has an ability to search online
9. Connects to social networking sites
10. Access infinite number of entertainment possibilities
11. Ability to enhance view with real time data related content

The users of Smart TV can store their personal and other data in the TV using the internal ram that serves as an on board memory. All the relevant data is stored here and this ram is not upgradable. The data can also be stored on the external hard drive or the cloud storage of the TV.

Data mining has been given a new meaning and dimension with the emergence of Smart TV in the world of technology. The TV can remember and capture user's viewing history, and combine the data of the viewer's view with the server's knowledge. All the information that is accumulated using the data and knowledge is sent and stored in TV maker's server [7]. The data

is chunked, and movie recommendation engine is built exactly like Netflix does. This also a way through which the viewer history is stored and used for further recommendations and updates. The TV is connected to the internet and data is stored in the cloud storage [7].

3 SMART TV AND CYBERCRIME

Cyber Crime (also called computer crime, hi-tech crime, and e-crime) is used to describe criminal activity in which computers or networks are a tool, a target, or a place of criminal activity. A few examples of cyber crime include: Theft of Intellectual Property, Identify Theft, Copyright Piracy, Child Pornography, Illegal Gambling, Planting of Virus and Worms, Storing Illegal Information, Hacking, Password Trafficking, Social Engineering and Fraud.

Smart TV has become the next target for the cyber crimes. The potential of smart TV to become a new source and avenue of access has increased for such illicit crimes. Smart TVs give suitable ways and methods to store data of all kinds, including all personal contents like images, video, audio and text files. They also provide a way for criminals to access, possess and hide illegal material too. Also, these smart devices are being used for hacking purposes to steal the personal information of the user [8]. The users are ignorant of such hacking and they seem to enjoy the technology without considering the security threats it could lead to [9,10].

According to Eddie Williams, the potential of attacks has increased with the emergence of smart TVs. Smart TVs have become vulnerable because it provides a reasons to attack a whole new group of preys that could easily be exploited for illicit means at the hands of the predators, none other than the hackers itself. Above all in future it is expected that smart phones will facilitate the users for online shopping on the TV itself thus the paid services serves a lucrative target to the attackers as it previously had on smart phones and PCs [10].

The hackers can also exploit the privacy of the users by intruding into the house through the camera and provide a way to burglars to rob the house. Thus everything related to the users becomes vulnerable and susceptible to hacking.

4 SMART TV FORENSICS

4.1 Smart TV and Digital Forensics

Digital forensics is a collection of specialized techniques, processes, and procedures used to preserve, extract, analyze, and present electronic evidence that is found in digital devices, often in relation to computer or cyber crime [11].

The National Institute of Standards and Technology, NIST, divide digital forensics investigation into four phases [11], which are briefly summarized below:

1. **Collection**: Identify, label, record and acquire data from possible sources, while preserving the integrity of the data.

2. **Examination**: Use manual and automated methods to assess and extract data of particular interest, while preserving the integrity of the data.

3. **Analysis**: Use legally justifiable methods and techniques to derive useful information.

4. **Reporting**: Describe actions used, explain how tools and procedures were selected, determine what other actions need to be performed, including forensic examination of additional data sources, securing identified vulnerabilities and improving existing security controls. Recommend improvements to policies, guidelines, procedures, tools and other aspects of the forensic process.

Smart TV Forensics is the science of recovering digital evidence from a smart TV under forensically sound conditions. It includes recovery and analysis of data from smart TV and its aim to catch the perpetrators of crimes that involve the use of smart TV.

There are various forensics information that we can extract out of a smart TV and include but not limited to the following:

1. Photos and sound files.
2. Web browsing activities.
3. Audio and video recording
4. Electronic documents
5. Internet settings
6. Emails, memos, calendar, etc.
7. User applications

Smart TV Forensics is still in its infancy and currently facing too many challenges**:**

- The majority of smart TV devices are not widely supported by forensic solutions.
- Ever-changing advancement of Smart TV devices increases the complexity of smart TV examinations.
- No single standardized approach to investigate smart TV.
- Smart TV Forensic tools, if there are any, are operate only on a particular platform, operating system, and specific hardware architecture.

4.2 Smart TV and Xbox

The Xbox gaming console was launched by Microsoft on November 15, 2001. The Xbox contained similar equipment as that in the PC: a hard drive, a DVD drive, dedicated graphics hardware with TV-out, Ethernet and USB [12]. With some features and vulnerability, Smart TV to some extent is similar to newly introduced X Box one through many aspects [13]:

- Both has storage to secure data
- Uses internet to access interactive features
- Access to full range of services
- Access to multimedia
- Access to entertainment using camera and microphone
- Runs multiple application on split screens
- Interactive communication with the device.

With such similarity between X box and Smart TV, we may try to reassign different techniques and tools that have been used in X Box forensics to be used to certain extent in Smart TV forensics.

4.3 Security Countermeasures for Smart TV

As stated earlier, Smart TV has become a new source of target for the cyber criminals. It has become a necessity to protect it from any misuse or harm in the hands of such criminals.

Anti viruses must be created and installed in the TV device to provide utmost protection to the TV when any unknown data tries to harm the TV. Other than this there should be an access for the user that can indicate the intrusion of any threat or virus that has the potential to harm the device. This will identify the user of the possible threat.

5 CONCLUSIONS

Smart TV is a new innovation that has attracted a mass of users around it with its interactive features. It has made everything look so easy with a click the whole world is before you with a reliable internet connection. With the exceptional features to communicate with the device and access different services it has also given rise to threats like hacking and other form of cybercrimes. Smart TV Forensics is the science of recovering digital evidence from a smart TV under forensically sound conditions. In this paper, we presented various issues and challenges to be faced by Smart TV Forensics as it is still in its infancy. Proper security countermeasures are proposed to detect/prevent any malicious action that is targeting the smart TV. This will enable protecting not only the device but also the privacy, information and assets of its users.

6 REFERENCES

1. Dave Evans: The Internet of Things: How the Next Evolution of the Internet Is Changing Everything: Cisco Internet Business Solutions Group (IBSG) (2011).
2. Linus Mähler Lundgren: An examination of Smart TV platforms (2011). Data retrieved from http://dinoprojektet.se/wp-content/uploads/2011/12/dinolabs-dohi-SmartTVs-eng.pdf on June 18th 2013.
3. Paul O'Donovan: Market Trends: Smart TVs Are the Focus of the TV Market, Worldwide, 2012: Gartner (2012).
4. John Leyden: Samsung's smart TVs 'wide open' to exploits: The downside to being 'more like a PC': The Register (2012). Data retrieved from http://www.theregister.co.uk/2012/12/12/smart_tv_pwned/ on June 17th 2013.
5. Kevin Smith: The 8 Best Smart TVs You Can Buy. Business insider Inc. (2013). Data retrieved from http://www.businessinsider.com/best-smart-tvs-2013-3?op=1 on June 19th 2013.
6. Nikos Sidiropoulos and Periklis Stefopoulos: Smart TV Hacking. Research Project (2013). Data retrieved from http://rp.delaat.net/2012-2013/p39/report.pdf on June17th 2013.
7. Junling Hu: Smart TV and Data Mining. About Data Mining. Data retrieved from http://www.aboutdm.com/2013/01/smart-tv-and-data-mining.html on June 18th 2013.
8. David Collins: XFT: a forensic toolkit for the original Xbox game console: International Journal of Electronic Security and Digital Forensics, Volume2 Issue2, pp. 199--205 (2009).
9. Taylor Armerding: Smart TV hack highlights risk of 'The Internet of Everything': TechHive (2012). Data retrieved from http://www.techhive.com/article/2020538/smart-tv-hack-highlights-risk-of-the-internet-of-everything.html on June 18th 2013.
10. IFA 2012: Cyber Criminals Focusing on Smart TVs: G Data (2012). Data retrieved from http://www.gdatasoftware.co.uk/es/about-g-data/press-center/news/article/article/2897-ifa-2012-cyber-criminals-focu.html on June 18th 2013.
11. Karen Kent, Suzanne Chevalier, Tim Grance and Hung Dang: Guide to Integrating

Forensic Techniques into Incident Responses: NIST Special Publication 800-86 (2006).
12. Philip Craiger and Paul Burke: Forensic Analysis of Xbox Consoles: In IFIP International Federation for Information Processing, Volume 242, no. 1 (2010).
13. Chris Gayomali: Is the Xbox One the smart TV we've all been waiting for? The Week (2013). Data retrieved from http://theweek.com/article/index/244515/is-the-xbox-one-the-smart-tv-weve-all-been-waiting-for on June 18th 2013.